User's Manual

11n WLAN Outdoor CPE

Model No.: SP9012N

V1.0 January 2010

Copyright

Copyright © 2010 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About This Manual

This user manual is intended to guide professional installer to install the SP9012N Outdoor Wireless CPE and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:

Note:

- This indicates an important note that you must pay attention to.

Warning:

- This indicates a warning or caution that you have to abide.

Bold: Indicates the function, important words, and so on.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding radio frequency exposure limits, you shall beep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Warranty

Micronet's standard hardware warranty is for one (1) year from date of shipment from Micronet or a Micronet Distributor. Micronet warrants that hardware will conform to the current relevant published specifications and will be free from material defects in material and workmanship under normal use and service.

IN NO EVENT SHALL MICRONET COMMUNICATION, INC. BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE RISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF MICRONET COMMUNICATION, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL MICRONET'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

Content

Chapter 1 Introduction 1

Introduction 1

Appearance 2

Key Features 2

Typical Application 2

Chapter 2 Hardware Installation 4

Preparation before Installation 4

Professional Installation Required 4

Safety Precautions 4

Installation Precautions 5

Product Package 5

Hardware Installation 7

Connect up 7

Pole Mounting 10

Using the External Antenna 12

Chapter 3 Basic Settings 13

Factory Default Settings 13

System Requirements 14

How to Login the Web-based Interface 14

Basic System Settings 16

Basic Wireless Settings 17

Site Survey 19

Chapter 4 Advanced Settings 20

Advanced Settings 20

RADIUS Settings 23

Security Settings 24

Security Settings 24

Access Control 26

Chapter 5 Management 27

View SP9012N Outdoor Wireless CPE Basic Information 27

Time Settings 28

SNMP Management 29

Configure SNMPv3 User Profile 30

Upgrade Firmware 32

Configuration File 33

Password Settings 35

View Network Flow Statistics 36

Association List 37

System Log 38

Chapter 6 Troubleshooting 39

Appendix A. ASCII 41

Appendix B. GPL Declamation 42

FIGURE

Figure 1 SP9012N Outdoor Wireless CPE 2
Figure 2 Typical Application 3
Figure 3 Move the Cover 7
Figure 4 Cable Connection 7
Figure 5 Seal the Bottom 8
Figure 6 Connect to PoE Injector 8
Figure 7 Complete Set 9
Figure 8 Pole Mounting – Step 1 10
Figure 9 Pole Mounting – Step 2 10
Figure 10 Pole Mounting – Step 3 11
Figure 11 Move the Rubber 12
Figure 12 Login Page 14
Figure 13 Main Page 15
Figure 14 Basic System Settings 16
Figure 15 Basic Wireless Settings 17
Figure 16 Site Survey 19
Figure 17 Advanced Wireless Settings 20
Figure 20 RADIUS Settings 23
Figure 18 Security Settings 24
Figure 19 Access Control 26
Figure 21 Basic Information 27
Figure 27 Time Settings 28
Figure 25 SNMP Configuration 29
Figure 26 Configure SNMPv3 User Profile 30
Figure 29 Upgrade Firmware 32
Figure 30 Backup/Retrieve Settings 33
Figure 28 Password 35
Figure 22 Network Flow Statistics 36
Figure 23 Connection 37

Figure 24 System Log 38

Figure 33 MAC Address 39

TABLE

Table 1 SP9012N Outdoor Wireless CPE Factory Default Settings 13

Table 2 ACSII 41

Table 3 Public Software Name and Description 43

Chapter 1 Introduction

Introduction

Designed for outdoor environment application, the SP9012N Outdoor Wireless CPE is a high-performance last-mile broadband solution that provides reliable wireless network coverage. As an IEEE 802.11b/g/n compliant wireless device, the SP9012N Outdoor Wireless CPE is able to give stable and efficient wireless performance, while designed with IEEE 802.11n draft 2.0 standard and high output power makes it possible to deliver several times faster data rate then normal wireless device and higher bandwidth with longer range for outdoor applications.

The SP9012N Outdoor Wireless CPE supports AP and Wireless Client dual wireless communication connectivity, allowing for various application requirements thus helping to find the key to the “last mile” with least effort.

With high output power and reliable performance, the SP9012N Outdoor Wireless CPE is an ideal wireless broadband solution for wireless Internet service providers and system integrators!

Appearance

Figure 1 SP9012N Outdoor Wireless CPE

Key Features

- Compliant with IEEE 802.11b/g and IEEE 802.11n draft 2.0 as well
- Support Power over Ethernet (PoE). * Only PoE injector with 12V output is able to be used with SP9012N Outdoor Wireless CPE.
- IP65 waterproof housing endures almost any harsh environments
- Dual operating modes including AP and Wireless Client
- Support 64/128-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK etc
- Support WMM and Quality of service (QoS) for enhanced performance
- Advanced management tools like SNMP
- User-friendly Web and SNMP-based management interface

Typical Application

This section describes the typical applications of SP9012N Outdoor Wireless CPE. By default, it is set

to AP mode which allows it to establish a wireless coverage for a small range of areas like campuses, squares, cafes, etc.; besides, it is also able to join any available wireless network under wireless client mode. The SP9012N Outdoor Wireless CPE is able to deliver stable and efficient broadband connectivity for various applications.

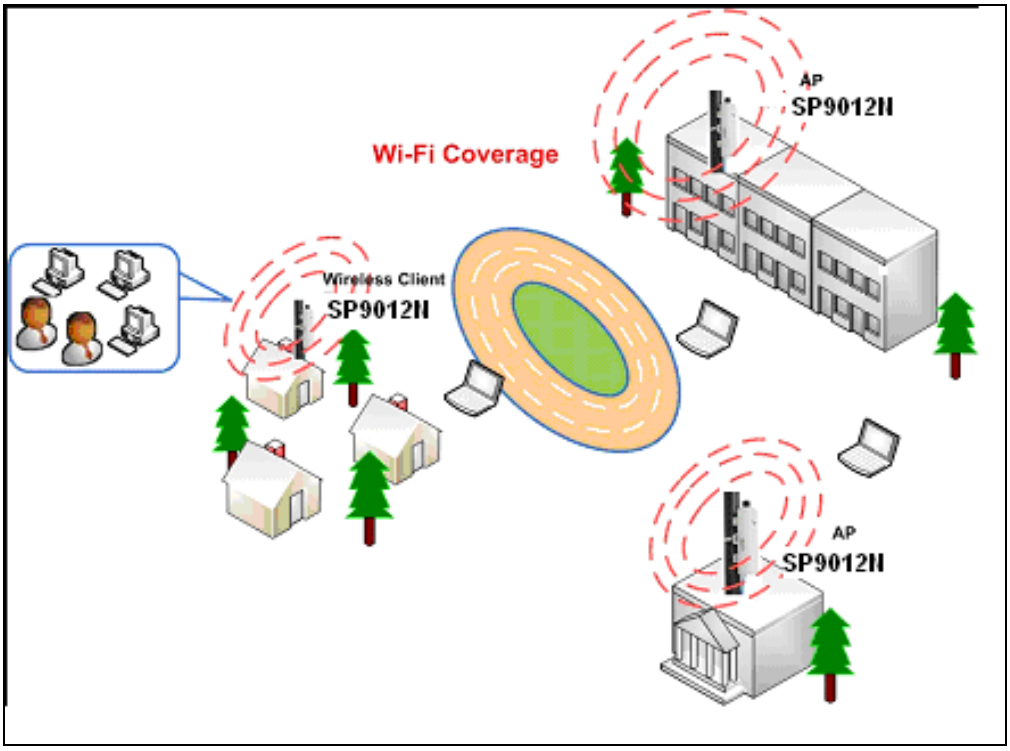

Figure 2 Typical Application

Besides, the SP9012N Outdoor Wireless CPE can also be applied into the following environments:

- Cost-effectively provide long distance backhaul for remote areas (e.g. village, oil well, island, mountain and etc.)
- Establish local backhaul for campus, farm and factory
- Provide and access for video streaming or surveillance for industrial and mining enterprises

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing SP9012N Outdoor Wireless CPE.

Preparation before Installation

Professional Installation Required

1. Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.
2. The SP9012N Outdoor Wireless CPE is distributed through distributors and system installers with professional technicians.

Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing SP9012N Outdoor Wireless CPE for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing SP9012N Outdoor Wireless CPE, please note the following things:
   - Do not use a metal ladder;
   - Do not work on a wet or windy day;
   - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

Installation Precautions

To keep the SP9012N Outdoor Wireless CPE well while you are installing it, please read and follow these installation precautions.

1. **Users MUST use a proper and well-installed surge arrestor and grounding kit with SP9012N Outdoor Wireless CPE; otherwise, a random lightening could easily cause fatal damage to SP9012N Outdoor Wireless CPE. EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.**
2. **Users MUST use the "Power cord & PoE Injector" shipped in the box with the SP9012N Outdoor Wireless CPE. Use of other options will cause damage to the SP9012N Outdoor Wireless CPE.**
3. **When you intend to use an external antenna with SP9012N Outdoor Wireless CPE, please power SP9012N Outdoor Wireless CPE off first, then install the external antenna, and finally power it on for further use. Please follow the steps as mentioned above; otherwise, damage might be caused to the SP9012N Outdoor Wireless CPE itself.**

Product Package

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

- SP9012N Outdoor Wireless CPE ×1
- Pole Mounting Ring ×1
- Power Cord & PoE Injector ×1
- Quick Installation Guide ×1
- Product CD ×1

Note:

- Product CD contains Quick Installation Guide and User Manual!

Pole Mounting Ring

Power Cord & PoE Injector

Warning:

- Users MUST use the “Power cord & PoE Injector” shipped in the box with the SP9012N Outdoor Wireless CPE. Use of other options will cause damage to the SP9012N Outdoor Wireless CPE.

Hardware Installation

Connect up

1. The bottom of the SP9012N Outdoor Wireless CPE is a movable cover. Grab the cover and pull it back harder to take it out as the figure shown below.

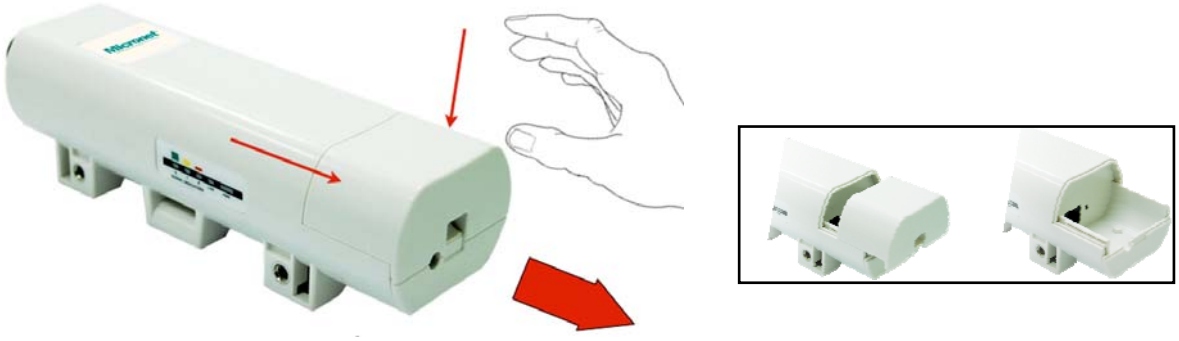

Figure 3 Move the Cover

2. Plug a standard Ethernet cable into the RJ45 port.

Figure 4 Cable Connection

3. Slide the cover back to seal the bottom of the SP9012N Outdoor Wireless CPE.

Figure 5 Seal the Bottom

4. Plug the power cord into the DC port of the PoE injector as the following right picture shows.

Figure 6 Connect to PoE Injector

5. Plug the other side of the Ethernet cable as shown in Step 3 into the PoE port of the PoE injector and get the complete set ready.

Figure 7 Complete Set

Pole Mounting

1. Turn the SP9012N Outdoor Wireless CPE over. Put the pole mounting ring through the middle hole of it. Note that you should unlock the pole mounting ring with a screw driver before putting it through SP9012N Outdoor Wireless CPE as the following right picture shows.

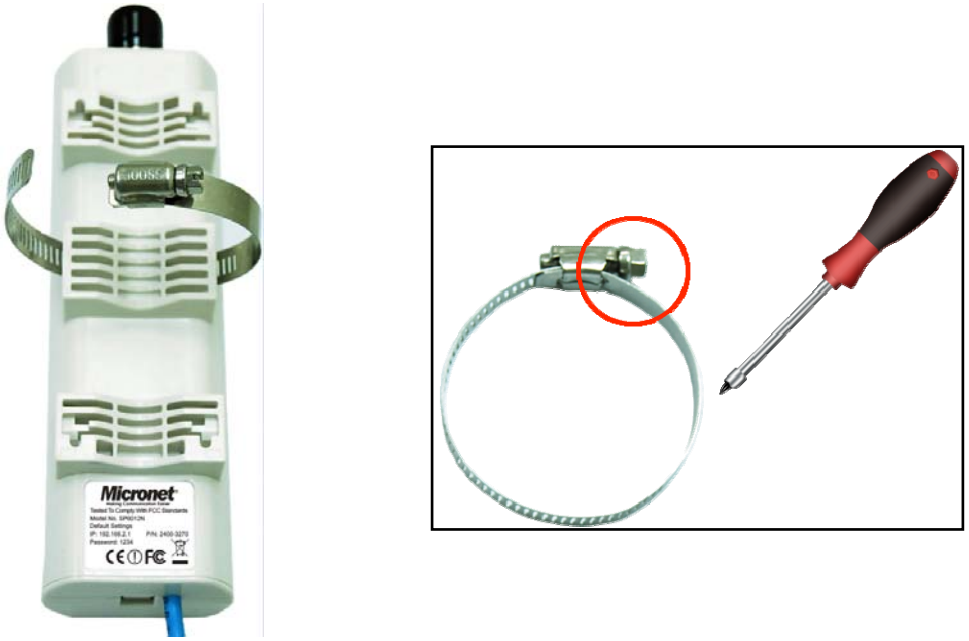

Figure 8 Pole Mounting – Step 1

2. Mount SP9012N Outdoor Wireless CPE steadily to the pole by locking the pole mounting ring tightly.

Figure 9 Pole Mounting – Step 2

3. Now you have completed the hardware installation of SP9012N Outdoor Wireless CPE.

Figure 10 Pole Mounting – Step 3

Using the External Antenna

If you prefer to use the external antenna with N-type connector for your application instead of the built-in directional antenna, please follow the steps below.

1. Grab the black rubber on the top of SP9012N Outdoor Wireless CPE, and slightly pull it up. The metal N-type connector will appear.

Figure 11 Move the Rubber

2. Connect your antenna with the N-type connector on the top of SP9012N Outdoor Wireless CPE.

Note:

- If you are going to use an external antenna on SP9012N Outdoor Wireless CPE, get some cable in advance.
- Be aware of the force you use while connecting to the N-type connector, inappropriate force may damage the N-type connector!

Warning:

- When you intend to use an external antenna with SP9012N Outdoor Wireless CPE, please power SP9012N Outdoor Wireless CPE off first, then install the external antenna, and finally power it on for further use. Please follow the steps as mentioned above; otherwise, damage might be caused to the SP9012N Outdoor Wireless CPE itself.

Chapter 3 Basic Settings

Factory Default Settings

We'll elaborate the SP9012N Outdoor Wireless CPE factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Table 1 SP9012N Outdoor Wireless CPE Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		1234
Wireless Device Name		apXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Operating Mode		AP
Data Rate		Auto
LAN	IP Address	192.168.2.1
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Spanning Tree		Enable
802.11 Mode		802.11b/g/n
Channel Number		Auto
SSID		Wireless
Broadcast SSID		Enable
HT Protect		Disable
Data Rate		Auto
Output Power		100% (Full)
Channel Mode		20MHz
WMM		Disable
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Beacon Interval		100
DTIM Interval		1
Space in Meter		0
Flow Control by AP		Disable
Uplink Speed Control(Tx)		1687
Security		Open System

Encryption		None
Wireless Separation		Disable
Access Control		Disable
SNMP	Enable/Disable	Enable
	Read Community Name	Public
	Write Community Name	Private
	IP Address	0.0.0.0

System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.2.x, as the default IP address of SP9012N Outdoor Wireless CPE is 192.168.2.1. (X cannot be 0, 1, nor 255);
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape or Firefox.

How to Login the Web-based Interface

SP9012N Outdoor Wireless CPE provides you with user-friendly Web-based management tool.

- Open IE and enter the IP address (Default: **192.168.2.1**) of SP9012N Outdoor Wireless CPE into the address field. You will see the login page as below.

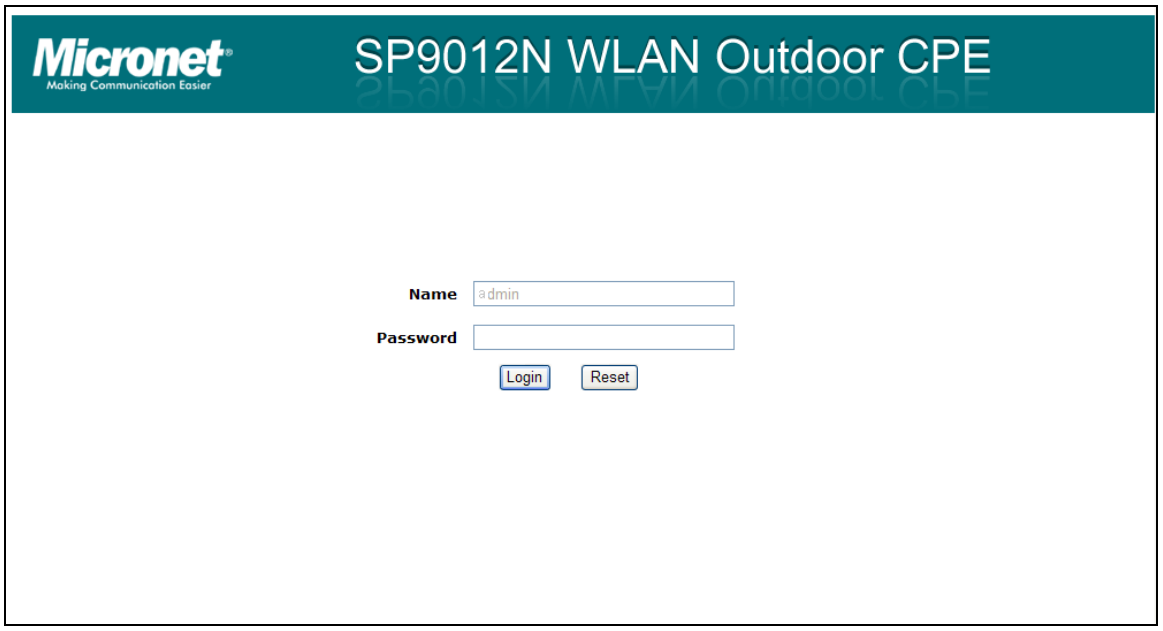

Figure 12 Login Page

- Enter the password (Default: 1234) and click "**Login**" to login the main page of SP9012N Outdoor Wireless CPE. As you can see, this management interface provides four main options in the black bar above, which are System, Wireless, Management and Statistics.

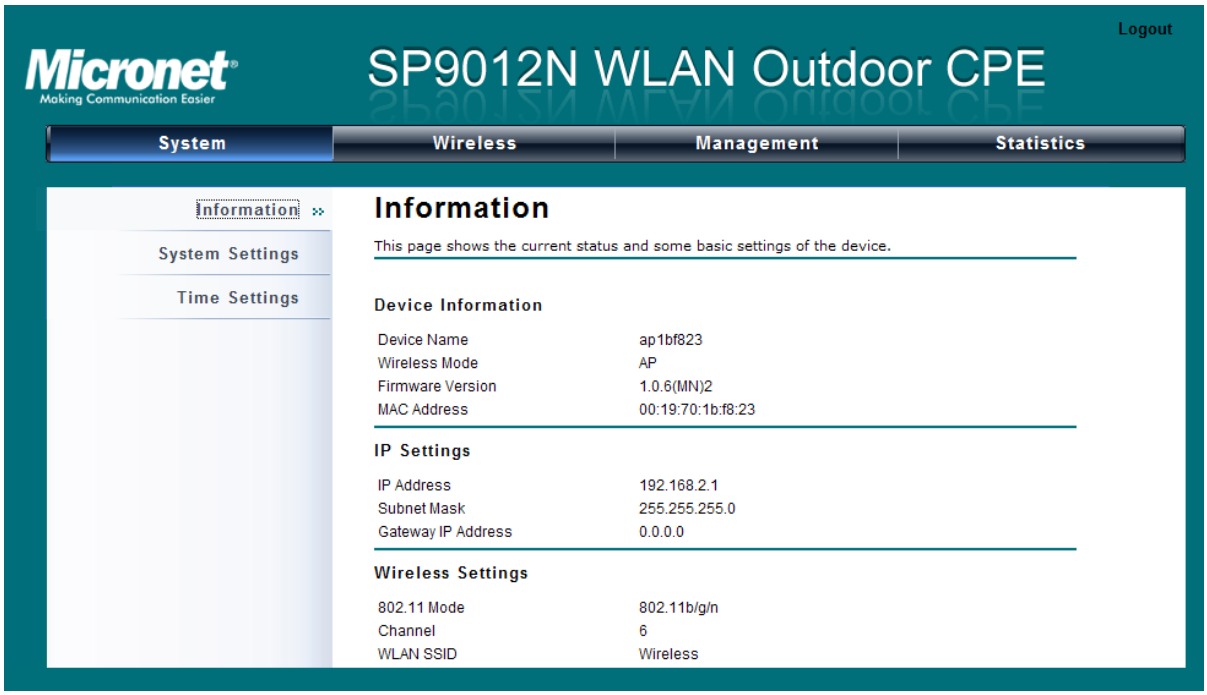

Figure 13 Main Page

Note:

- The username and password are case-sensitive, and the password should be no more than 19 characters!

Basic System Settings

For users who use the SP9012N Outdoor Wireless CPE for the first time, it is recommended that you begin configuration from "**System Settings**" in "**System**" shown below:

Figure 14 Basic System Settings

- **Device Settings**

  Device Name: Specify the device name for recognition, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-). Device Name provides users with another option to view the login webpage; in other words, open IE, enter the Device Name (ex: ap243943) of SP9012N Outdoor Wireless CPE into the address field, click enter, and then login webpage will show up.

- **IP Address Assignment**

  Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the SP9012N Outdoor Wireless CPE is able to obtain IP settings automatically from that DHCP server.

  Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for SP9012N Outdoor Wireless CPE manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

- **Spanning Tree**

  Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

- **Enable MAC Clone**

  Available only under wireless client mode, it hides the MAC address of the AP while displays the one of associated wireless client or the MAC address designated manually.

Basic Wireless Settings

Open "**Basic Settings**" in "**Wireless**" as below to make basic wireless configuration.

Figure 15 Basic Wireless Settings

- **Disable Wireless LAN Interface**

  Check this option to disable WLAN interface, then the wireless module of SP9012N Outdoor Wireless CPE will stop working and no wireless device can connect to it.

- **Wireless Mode**

  Two operating modes are available on SP9012N Outdoor Wireless CPE.

  Wireless Client: The SP9012N Outdoor Wireless CPE is able to connect to the AP and thus join the wireless network around it.

  AP: The SP9012N Outdoor Wireless CPE establishes a wireless coverage and receives connectivity from other wireless devices.

- **Wireless Network Name (SSID)**

  This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and can not exceed 32 characters.

- **Broadcast SSID**

  Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA can not scan and find SP9012N Outdoor Wireless CPE, so that malicious attack by some illegal STA could be avoided.

- **802.11 Mode**

  The SP9012N Outdoor Wireless CPE can communicate with wireless devices of 802.11b/g or 802.11b/g/n. You can also select Auto and make it work under an appropriate wireless mode automatically.

- **HT Protect**

  Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

- **Channel Number**

  Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

- **Antenna**

  By default, SP9012N Outdoor Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from “Internal (8 dBi)” to”External (N-Type)”.

Note:

- You are able to choose “External (N-Type)” only when you have well done installing the external antenna; otherwise, it might hurt SP9012N Outdoor Wireless CPE itself.

- **Output Power**

  Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. Usually “**Full**” is preferred.

- **Data Rate**

  Usually "**Auto**" is preferred. Under this rate, the SP9012N Outdoor Wireless CPE will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Channel Mode**

  Two levels are available: 20MHz and 40MHz. The latter one can enhance the data rate more effectively, but takes more bandwidth, thus cause potential interference.

- **Extension Channel Protection Mode**

  This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Site Survey

Under wireless client mode, the SP9012N Outdoor Wireless CPE is able to perform site survey, through which, information on the available access points will be detected.

Open "**Basic Settings**" in "**Wireless**", by clicking the "**Site Survey**" button beside "**Wireless Mode**" option, the wireless site survey window will popup with a list of available wireless networks around. Select the AP you would like to connect and click "**Selected**" to establish connection.

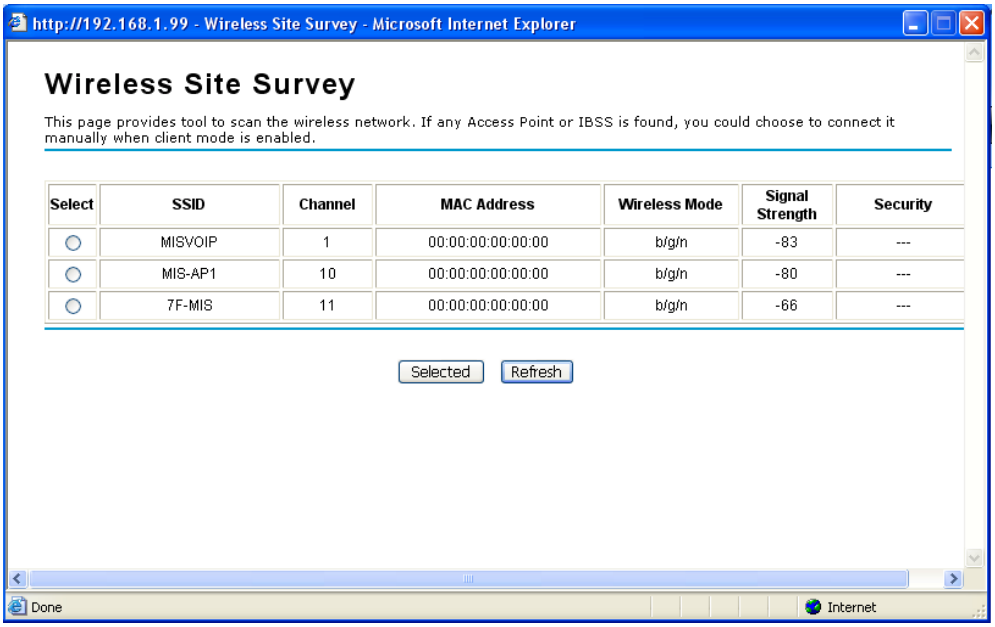

Figure 16 Site Survey

Chapter 4 Advanced Settings

Advanced Settings

Open “**Advanced Settings**” in “**Wireless**” to make advanced wireless settings.

Logout
Micronet
Making Communication Easier
SP9012N WLAN Outdoor CPE
System
Wireless
Management
Statistics
Basic Settings
Advanced Settings
RADIUS Settings
Security Settings
Access Control
Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will take.
WMM Support: Enabled Disabled
A-MPDU aggregation Enabled Disabled
A-MSDU aggregation Enabled Disabled
Short GI Enabled Disabled
RTS Threshold: 2346 (1-2346)
Fragment Threshold: 2346 (256-2346)
Beacon Interval: 100 (20-1024 ms)
DTIM Interval: 1 (1-255)
Preamble Type: Long Short
IGMP Snooping: Enabled Disabled
Wireless Separation: Enabled Disabled

Figure 17 Advanced Wireless Settings

- **WMM Support**

  WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should support it.

- **A-MPDU/A-MSDU Aggregation**

  Under AP mode, the data rate of your AP could be enhanced greatly with this option enabled; however, if your wireless clients don’t support A-MPDU/A-MSDU aggregation, it is recommended not to enable it.

- **Short GI**

  Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

- **RTS Threshold**

  The SP9012N Outdoor Wireless CPE sends RTS (Request to Send) frames to certain receiving

station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte.

- **Fragmentation Length**

  Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Beacon Interval**

  Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

- **DTIM Interval**

  DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

- **Preamble Type**

  It defines some details on the 802.11 physical layer. "**Long**" and "**Short**" are available.

- **IGMP Snooping**

  IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

- **Wireless Separation**

  Wireless separation is an ideal way to enhance the security of network transmission. Under the AP mode, enable "**Wireless Separation**" can prevent the communication among associated wireless clients.

- **RIFS**

  RIFS (Reduced Inter Frame Spacing) is a means of reducing overhead and thereby increasing network efficiency.

- **Space in Meter**

  To reduce the chances of data retransmission at long distance, the SP9012N Outdoor Wireless CPE can automatically adjust proper ACK timeout value by specifying distance of the two nodes. The distance to be entered here is calculated in terms of meters, so if the actual distance between

two nodes is 5Km, please enter 5000 in the blank.

- **Flow Control by AP**

  Flow control helps keep stable communication and improve efficiency of the network if necessary.

- **Uplink Speed Control (Tx)**

  Specify fractional data rates (× 64Kbps). It allows the administrator to control the amount of data rate each user is receiving. This is only available in AP mode.

Note:

- We strongly recommended you leave most advanced settings at their defaults except Distance in Meters; any modification on them may negatively impact the performance of your wireless network.

RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.

Open "**RADIUS Settings**" in "**Wireless**" to make RADIUS configuration.

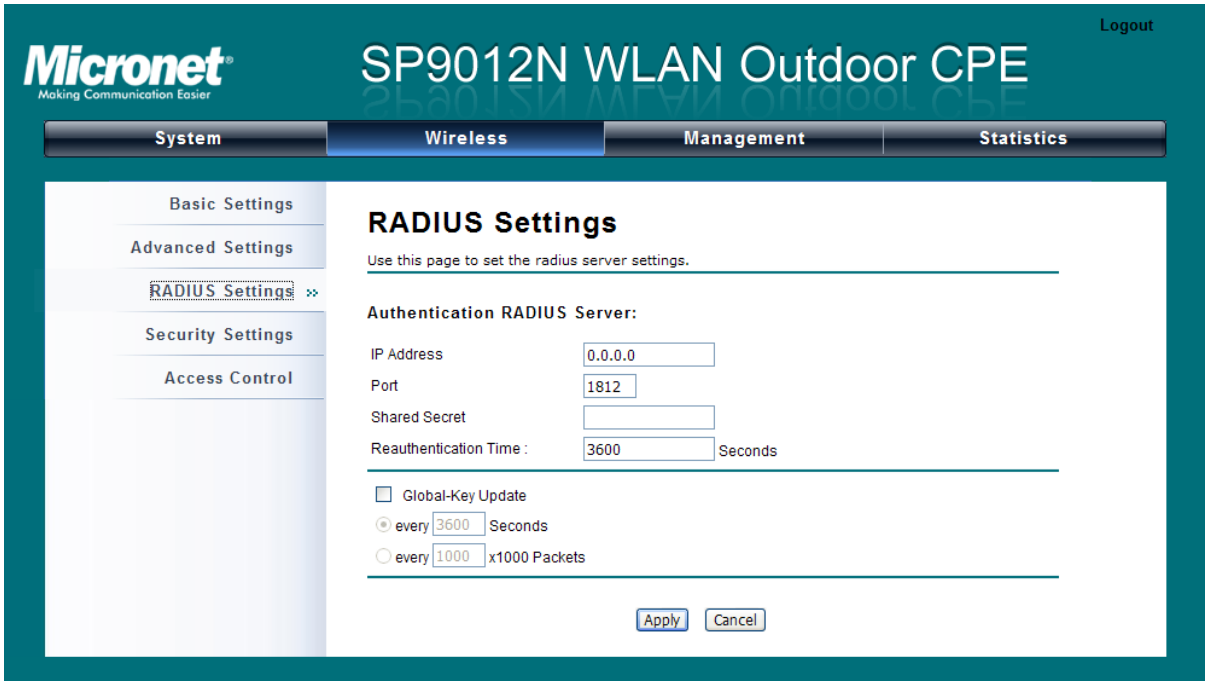

Figure 18 RADIUS Settings

- **Authentication RADIUS Server**

  This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

  IP Address: Enter the IP address of the Radius Server;

  Port: Enter the port number of the Radius Server;

  Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the SP9012N Outdoor Wireless CPE and RADIUS during authentication.

  Re-authentication Time: Set the time interval between two authentications.

  Global-Key Update: Check this option and specify the time interval between two global-key updates.

Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, the SP9012N Outdoor Wireless CPE provides you with rock solid security settings.

Security Settings

Open "**Security Settings**" in "**Wireless**" as below:

Figure 19 Security Settings

- **Network Authentication**

  Open System: It allows any device to join the network without performing any security check.

  Shared Key: Data encryption and key are required for wireless authentication.

  Legacy 802.1x: As an IEEE standard for port-based Network Access Control, it provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.

  WPA with RADIUS: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

  WPA2 with RADIUS: As a new version of WPA, only all the clients support WPA2, can it be

available. If it is selected, AES encryption and RADIUS server is required.

WPA&WPA2 with RADIUS: It provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.

WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: It provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

- **Data Encryption**

If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers or 5 ASCII characters.

128 bits WEP: It is made up of 26 hexadecimal numbers or 13 ASCII characters.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: It allows for backwards compatibility with devices using TKIP.

Note:

- We strongly recommend you enable wireless security on your network!
- Only setting the same Authentication, Data Encryption and Key in the SP9012N Outdoor Wireless CPE and other associated wireless devices, can the communication be established!

Access Control

The Access Control appoints the authority to wireless client on accessing SP9012N Outdoor Wireless CPE, thus a further security mechanism is provided. This function is available only under AP mode.

Open “**Access Control**” in “**Wireless**” as below.

Figure 20 Access Control

- **Access Control Mode**

  If you select “**Allow Listed**”, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when “**Deny Listed**” is selected, those wireless clients on the list will not be able to connect the AP.

- **MAC Address**

  Enter the MAC address of the wireless client that you would like to list into the access control list, click “**Apply**” then it will be added into the table at the bottom.

- **Delete Selected/All**

  Check the box before one or more MAC addresses of wireless client(s) that you would like to cancel, and click “**Delete Selected**” or “**Delete All**” to cancel that access control rule.

Chapter 5 Management

View SP9012N Outdoor Wireless CPE Basic Information

Open “**Information**” in “**System**” to check the basic information of SP9012N Outdoor Wireless CPE, which is read only. Click “**Refresh**” at the bottom to have the real-time information.

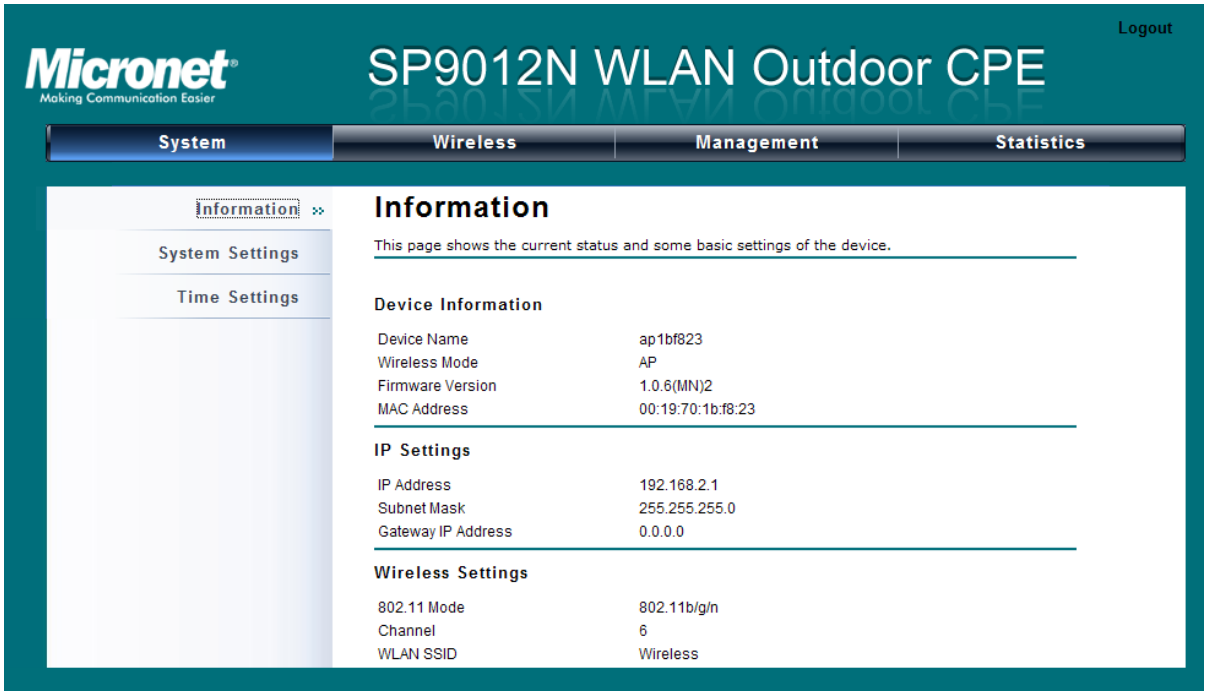

Figure 21 Basic Information

Time Settings

Compliant with NTP, the SP9012N Outdoor Wireless CPE is capable of keeping its time in complete accord with the Internet time. Make configuration in "**Time Settings**" from "**System**". To use this feature, check "**Enable NTP Client Update**" in advance.

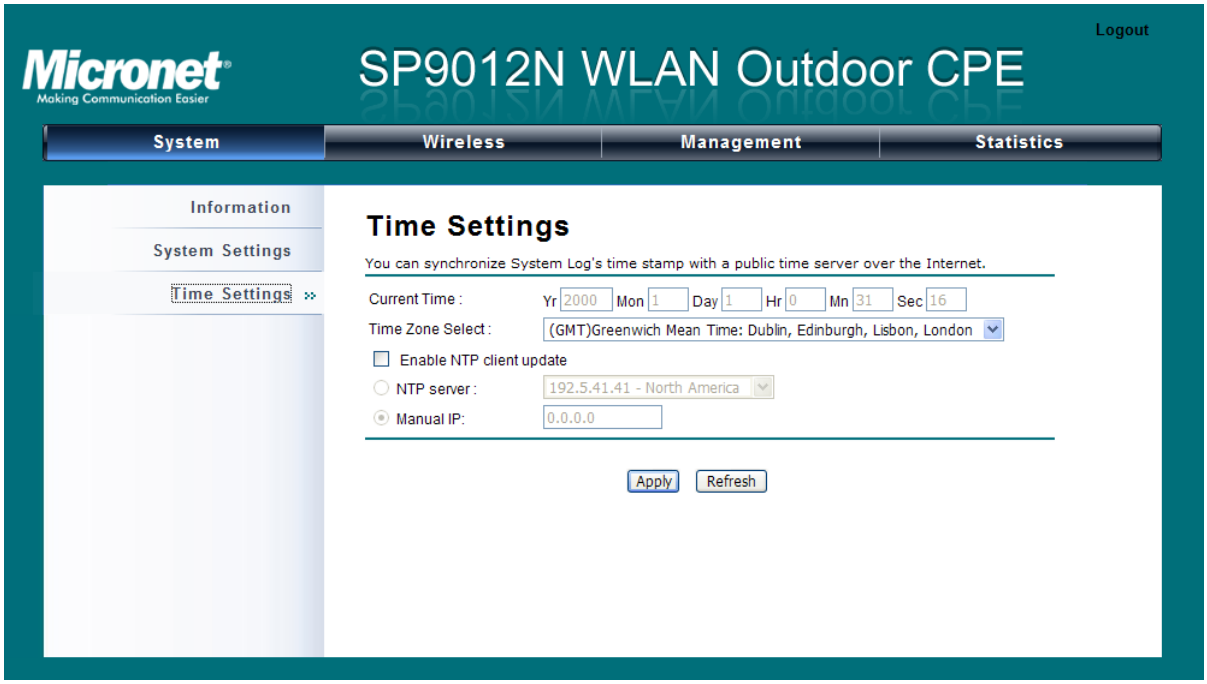

Figure 22 Time Settings

- **Time Zone Select**

  Select the time zone from the dropdown list.

- **NTP Server**

  Select the time server from the "**NTP Server**" dropdown list or manually input the IP address of available time server into "**Manual IP**".

  Hit "**Apply**" to save settings.

SNMP Management

The SP9012N Outdoor Wireless CPE supports SNMP for convenient remote management. Open "**SNMP Configuration**" in "**Management**" shown below. Set the SNMP parameters and obtain MIB file before remote management.

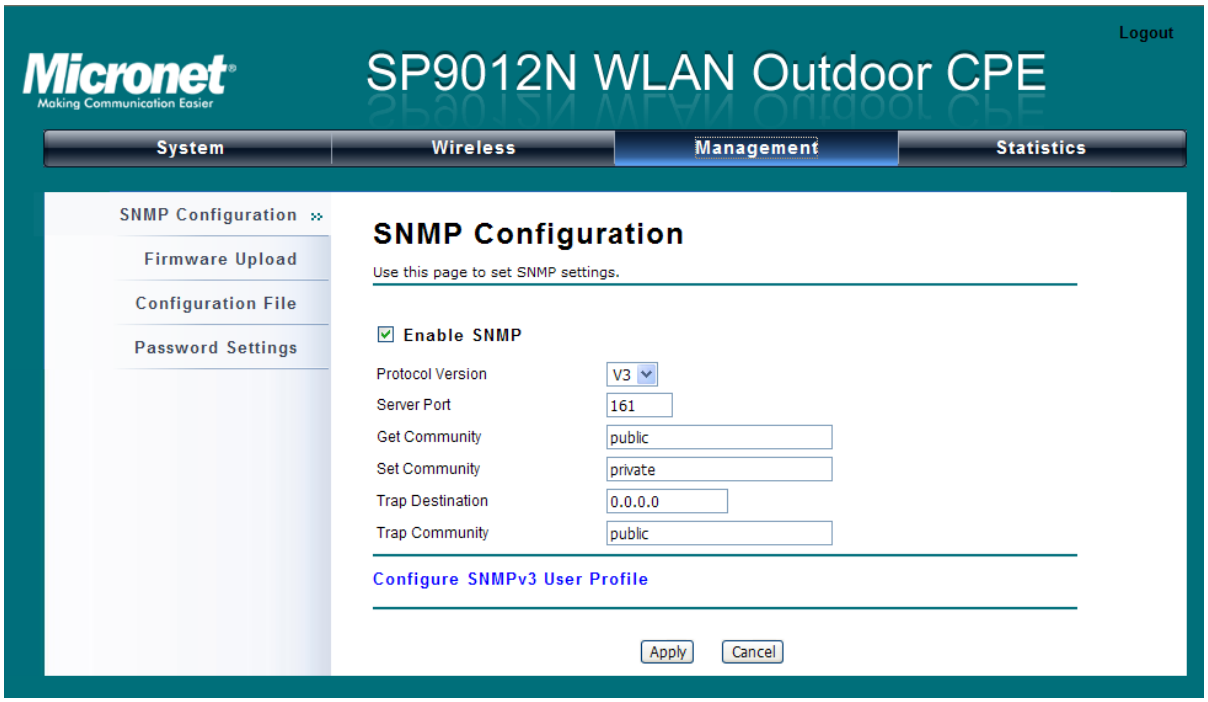

Figure 23 SNMP Configuration

- **Enable SNMP**

  Check this box to enable SNMP settings.

- **Protocol Version**

  Select the SNMP version, and keep it identical on the SP9012N Outdoor Wireless CPE and the SNMP manager.

- **Server Port**

  Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

- **Get Community**

  Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

- **Set Community**

  Specify the password for the incoming Set requests from the management station. By default, it is

set to private.

- **Trap Destination**

  Specify the IP address of the station to send the SNMP traps to.

- **Trap Community**

  Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

Configure SNMPv3 User Profile

For SNMP protocol version 3, you can click "**Configure SNMPv3 User Profile**" in blue to set the details of SNMPv3 user. Check "**Enable SNMPv3 Admin/User**" in advance and make further configuration.

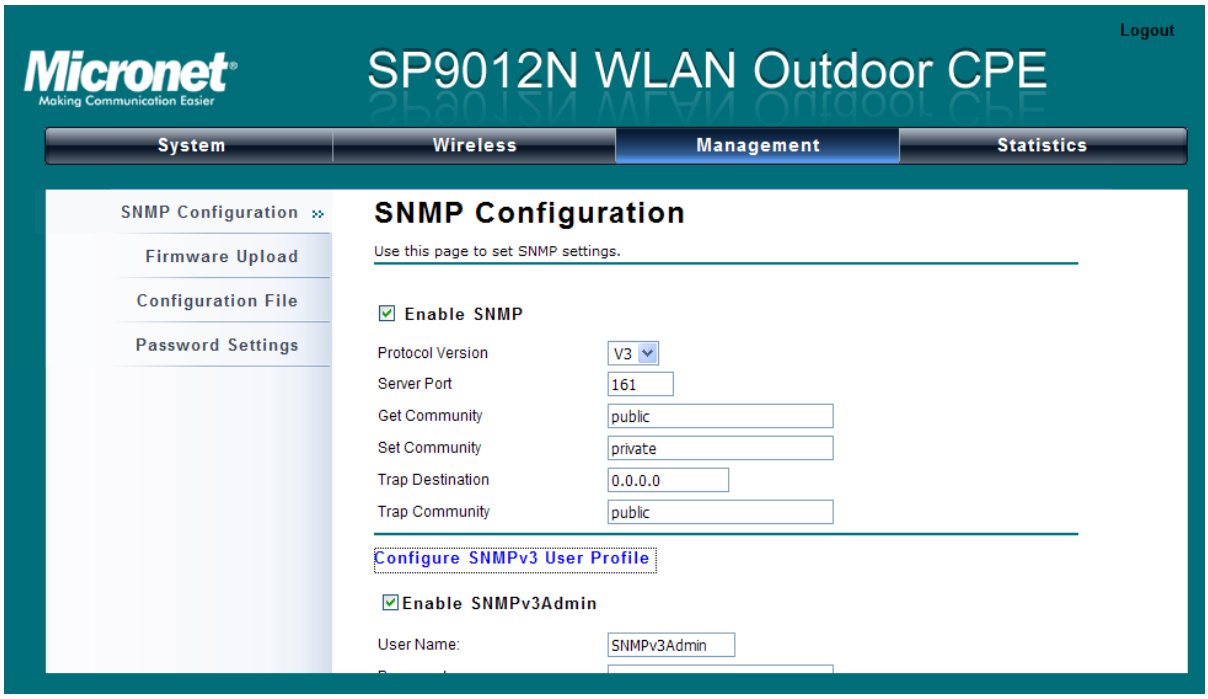

Figure 24 Configure SNMPv3 User Profile

- **User Name**

  Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the SP9012N Outdoor Wireless CPE.

- **Password**

  Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the SP9012N Outdoor Wireless CPE.

- **Confirm Password**

Input that password again to make sure it is your desired one.

- **Access Type**

  Select “**Read Only**” or “**Read and Write**” accordingly.

- **Authentication Protocol**

  Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

- **Privacy Protocol**

  Specify the encryption method for SNMP communication. None, DES and None are available.

  None: No encryption is applied.

  DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

Upgrade Firmware

Open “**Firmware Upload**” in “**Management**” and follow the steps below to upgrade firmware locally or remotely through SP9012N Outdoor Wireless CPE’s Web:

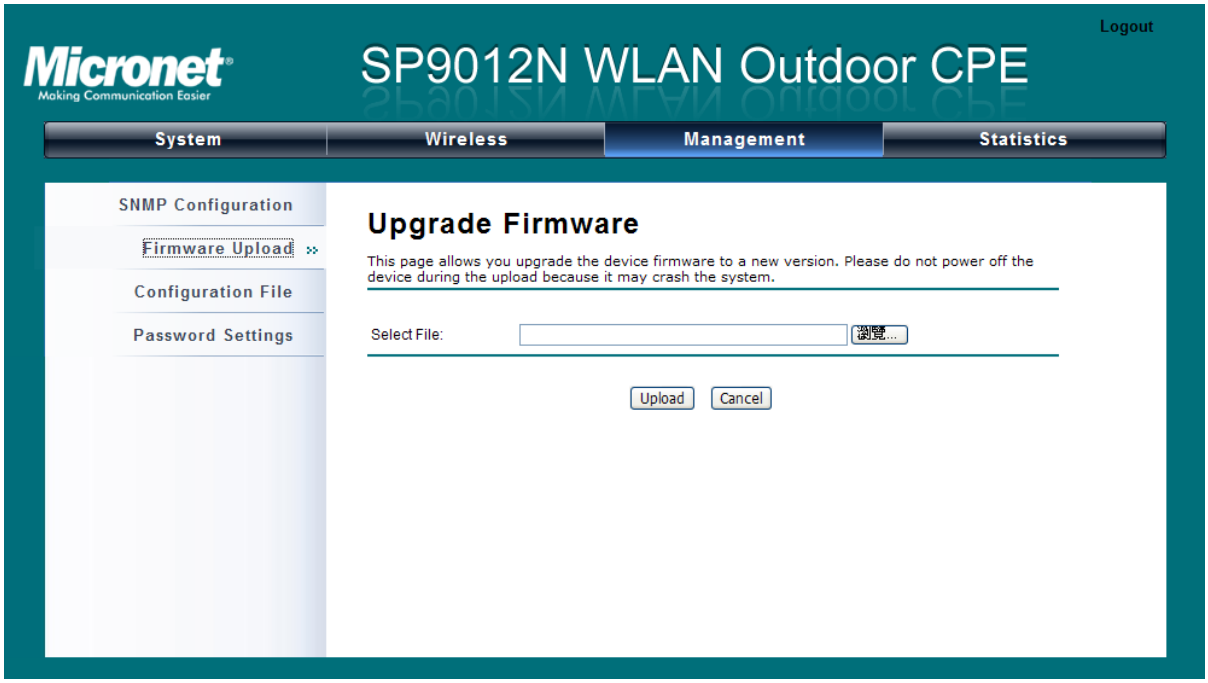

Figure 25 Upgrade Firmware

- Click “**Browse**” to select the firmware file you would like to load;
- Click “**Upload**” to start the upload process;
- Wait a moment, the system will reboot after successful upgrade.

Note:

- Do NOT cut the power off during upgrading; otherwise the system may severely crash!

Configuration File

Open “**Configuration File**” in “**Management**” as below:

Figure 26 Backup/Retrieve Settings

- **Save Settings to File**

  By clicking “**Save**”, a dialog box will popup. Save it, then the configuration file like ap.cfg will be saved to your local computer.

- **Load Settings from File**

  By clicking “**Browse**” a file selection menu will appear, select the file you want to load, like ap.cfg; Click “**Upload**” to load the file. After automatically rebooting, new settings are applied.

- **Reset Settings to Default**

  From “**Configuration File**”, clicking “**Reset**” will eliminate all current settings and reboot your device, then default settings are applied.

- **Reboot The Device**

  Click “**Reboot**” and hit “**Yes**” upon the appeared prompt to start reboot process. This takes a few minutes.

In addition, the SP9012N Outdoor Wireless CPE provides another way to restore the factory default settings:

- **Restore factory default settings via RS-232**

  If software in SP9012N Outdoor Wireless CPE is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button.

Password Settings

From “**Password Settings**” in “**Management**”, you can change the password to manage your SP9012N Outdoor Wireless CPE.

Enter the new password respectively in “**New Password**” and “**Confirm Password**” fields; click “**Apply**” to save settings.

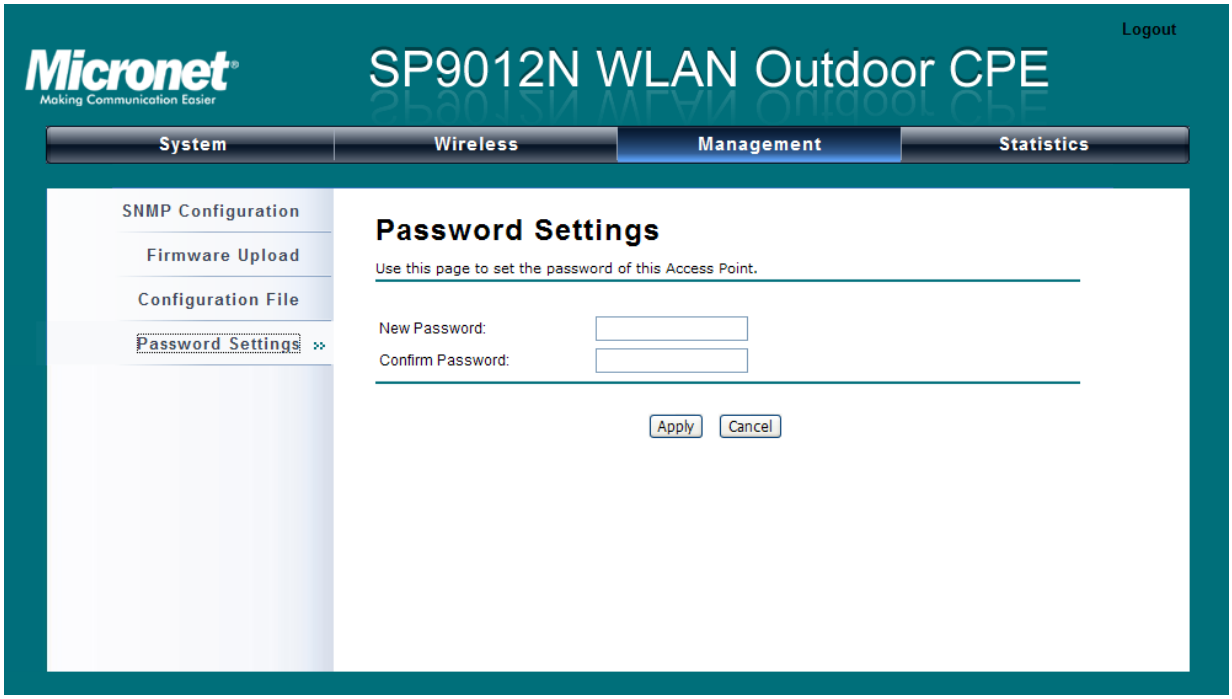

Figure 27 Password

Note:

- The password is case-sensitive and its length can not exceed 19 characters!

View Network Flow Statistics

Open “**Network Flow**” in “**Statistics**” to check the data packets received on and transmitted from the wireless and Ethernet ports. Click “**Refresh**” to view current statistics.

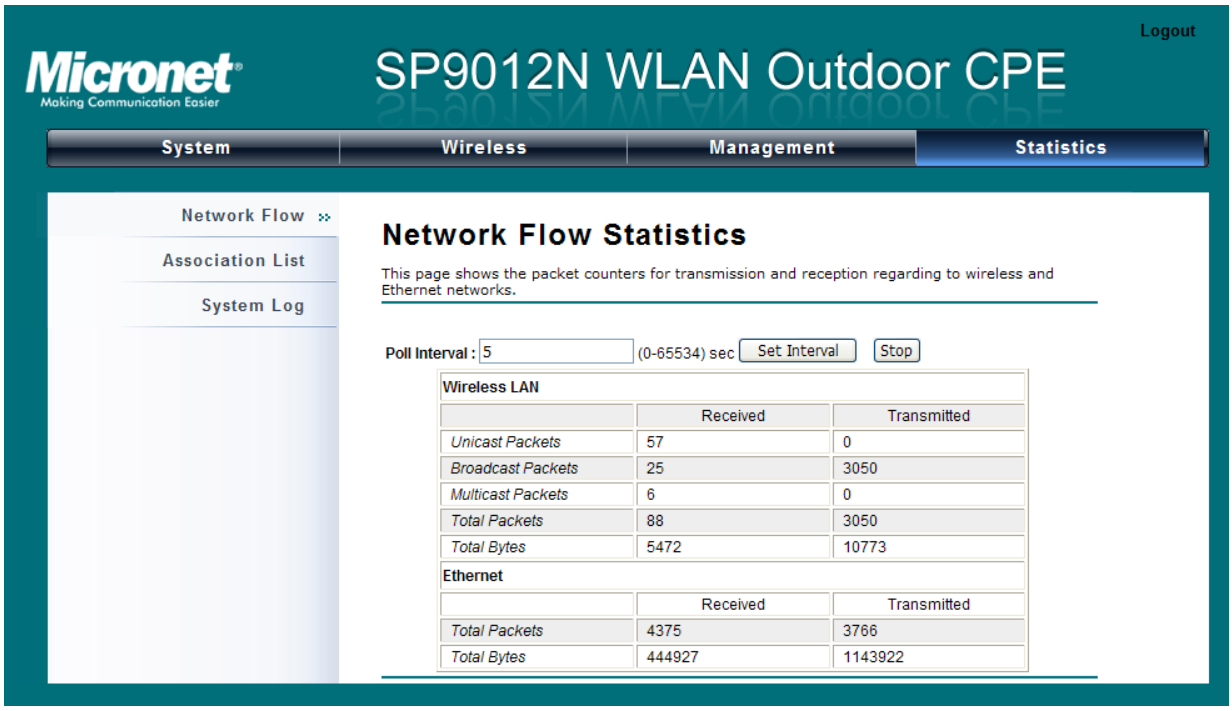

Figure 28 Network Flow Statistics

- **Poll Interval**

  Specify the refresh time interval in the box beside “**Poll Interval**” and click “**Set Interval**” to save settings. “**Stop**” helps to stop the auto refresh of network flow statistics.

Association List

Open “**Association List**” in “**Statistics**” to check the information of associated wireless clients. All is read only.

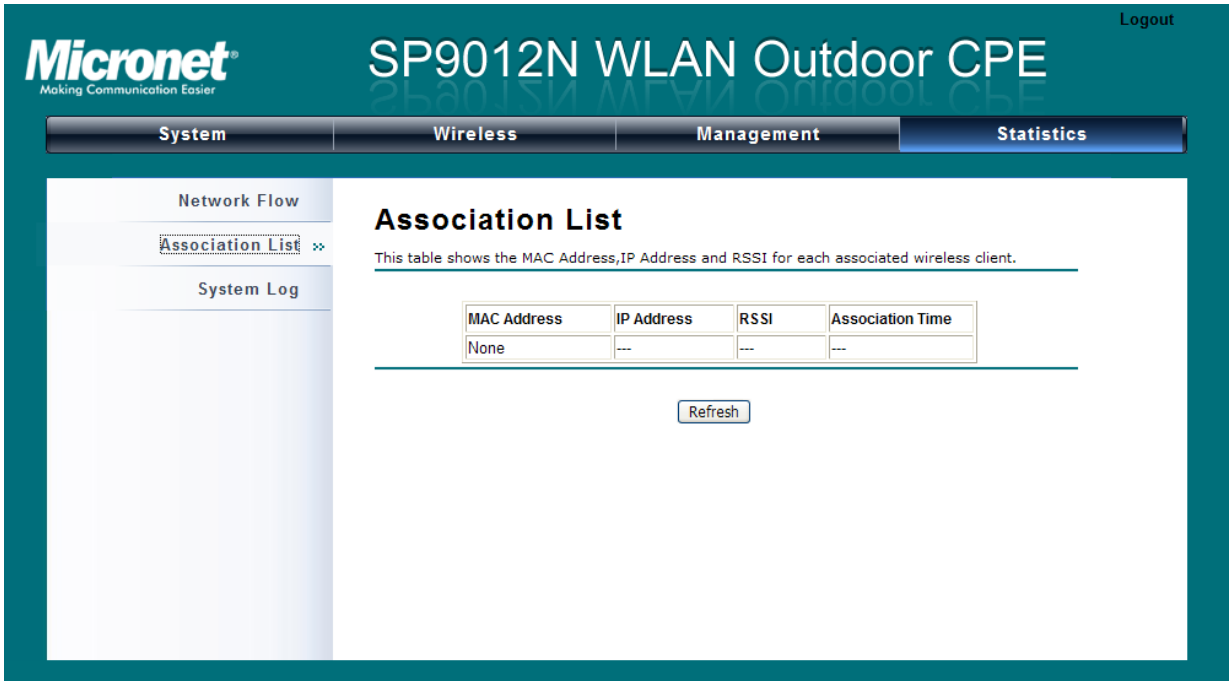

Figure 29 Connection

System Log

System log is used for recording events occurred on the SP9012N Outdoor Wireless CPE, including station connection, disconnection, system reboot and etc.

Open “**System Log**” in “**Statistics**” as below.

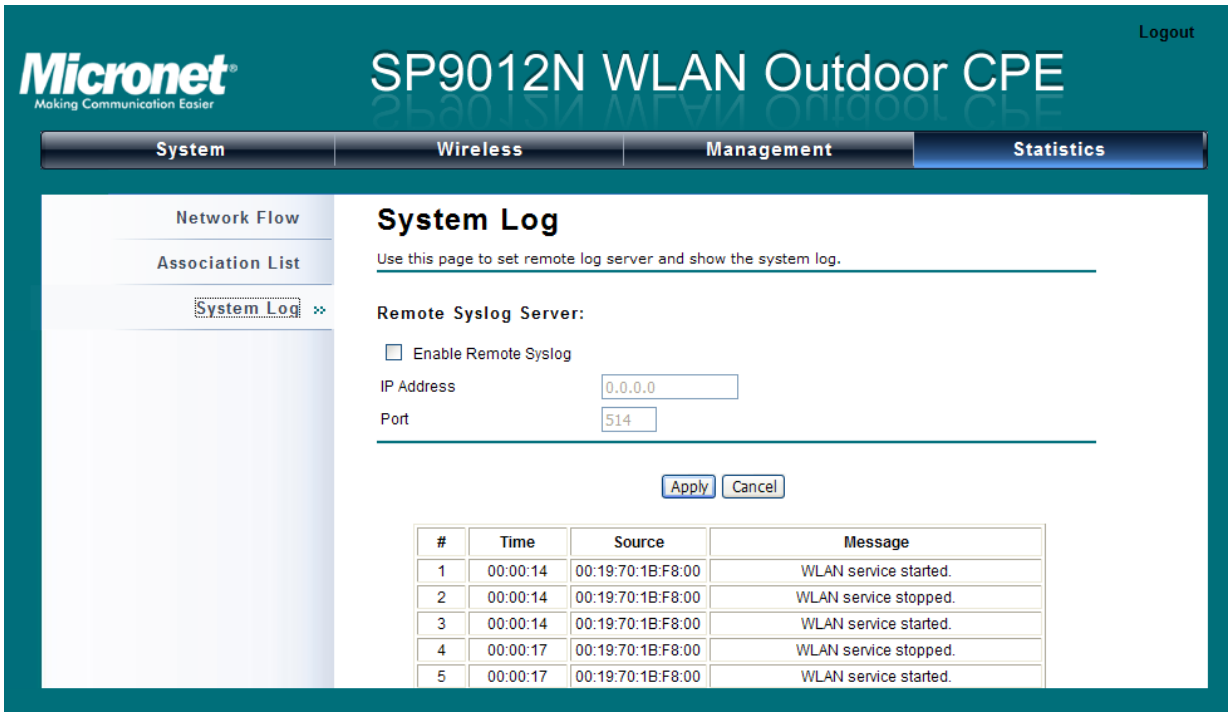

Figure 30 System Log

- **Remote Syslog Server**

  Enable Remote Syslog: Enable System log or not.

  IP Address: Specify the IP address of the server.

  Port: Specify the port number of the server.

Chapter 6 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the SP9012N Outdoor Wireless CPE. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of SP9012N Outdoor Wireless CPE?

MAC Address distinguishes itself by the unique identity among network devices. There are two ways available to know it.

- Each device has a label posted with the MAC address. Please refer below.

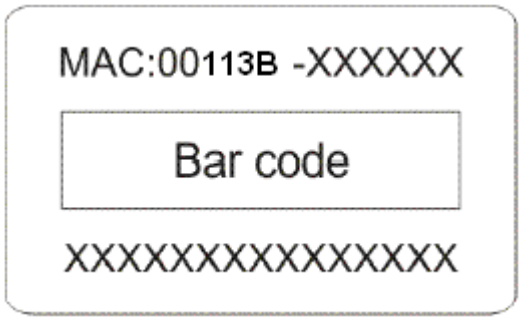

Figure 31 MAC Address

- On the SP9012N Outdoor Wireless CPE Web-based management interface, you can view the MAC Address from "View SP9012N Outdoor Wireless CPE Basic Information".

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in "**Configuration File**" from "**Management**" or by doing hardware reset via the reset button.

Q 3. What if I would like to backup and retrieve my configuration settings?

You may do the backup by generating a configuration file or retrieve the settings you have backed up previously in "**Configuration File**" from "**Management**".

Q 4. What if I can not access the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.
- Check whether the IP address of PC is correct (in the same network segment as the unit);
- Login the unit via other browsers such as Firefox.

- Hardware reset the unit.

Q 5. What if the wireless connection is not stable after associating with an AP under wireless client mode?

- Since the SP9012N Outdoor Wireless CPE comes with a built-in directional antenna, it is recommended make the SP9012N Outdoor Wireless CPE face to the direction where the AP is to get the best connection quality.
- In addition, you can start "**Site Survey**" in "**Wireless Basic Settings**" to check the signal strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available AP for better connection.

Appendix A. ASCII

WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal number or ACSII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

Table 2 ACSII

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
‘	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64	|	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Appendix B. GPL Declamation

PUBLIC SOFTWARE DECLAMATION

In the software we delivered, there may contains some public software, if it is, please read below carefully:

1. Definition

"**Public Software**", when applicable, shall mean that portion of the Licensed Software, in source code form, set forth in the below Table, and provided under the terms set forth in the Section 5, the indicated website, the complete license terms can be found.

"Public Software" shall mean each of:

(a) any computer code that contains, or is derived in any manner (in whole or in part) from, any computer code that is distributed as open source software (e.g. Linux) or similar licensing or distribution models; and

(b) any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software (i) be disclosed or distributed in source code form, (ii) be licensed for the purpose of making derivative works, or (iii) be redistributable at no charge.

Public Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (1) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (2) the Artistic License (e.g., PERL); (3) the Mozilla Public License; (4) the Netscape Public License; (5) the Sun Community Source License (SCSL); (6) the Sun Industry Source License (SISL); and (7) the Apache Software license.

2. Limited Use

Any Public Software provided under the agreement shall be subject to the licenses, terms and conditions of its model. Licensee hereby agrees to comply with the terms and conditions applicable to any such Public Software, as set forth in its presentation on website.

3. Limited Liability

The supplier hereby express that the supplier shall have no liability for any costs, loss or damages resulting from Licensee's breach of the terms and conditions applicable to use, conversion or combination of the licensed software with or into Public Software.

4. NO WARRANTY

This program or licensed software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY. THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH LICENSEE.

5. Public Software Name and Description

Table 3 Public Software Name and Description

Program Name	Copy Right Description	Origin Sour Code	Licenses or Distribution Models or its special license terms	License Terms Website Reference
Redboot	**Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003 Red Hat, Inc.**	**ftp://ftp.ges.redhat.com/private/gnupro-xscale-030422/redboot-intel-xscale-030630.tar.Z**	**eCos License**	**http://sources.redhat.com/ecos/ecos-license/**
Busybox		**http://www.busybox.net/downloads/busybox-1.01.tar.bz2**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**
brctl	**Copyright (C) 2000 Lennert Buytenhek**	**http://nchc.dl.sourceforge.net/sourceforge/bridge/bridge-utils-**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**

		1.0.6.tar.gz		
dropbear	**Copyright (c) 2002-2006 Matt Johnston Portions copyright (c) 2004 Mihnea Stoenescu**	**http://matt.ucc.asn.au/dropbear/dropbear-0.51.tar.bz2**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**
hostapd	**Copyright (c) 2002-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors**	**http://hostap.epitest.fi/releases/hostapd-0.4.8.tar.gz**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**
wpa_supplicant	**Copyright (c) 2003-2005, Jouni Malinen <jkmaline@cc.hut.fi> and contributors**	**http://hostap.epitest.fi/releases/wpa_supplicant-0.4.7.tar.gz**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**
mtdutil		**ftp://ftp.uk.linux.org/pub/people/dwmw2/mtd/cvs/mtd/util/**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**
ntpclient	**Copyright 1997, 1999, 2000, 2003 Larry Doolittle**	**http://doolittle.icarus.com/ntpclient/ntpclient_2003_194.tar.gz**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**
procps	**Author: Albert Cahalan, Michael K. Johnson, Jim Warner, etc.**	**http://procps.sourceforge.net/procps-3.2.7.tar.gz**	**GNU GENERAL PUBLIC LICENSE Version 2 GNU LIBRARY GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html http://www.gnu.org/licenses/old-licenses/library.html**
vsftpd	**Author: Chris Evans**	**ftp://vsftpd.beasts.org/users/cevans/vsftpd-1.1.2.tar.gz**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**

linux		**ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.20.3.tar.bz2**	**GNU GENERAL PUBLIC LICENSE Version 2**	**http://www.gnu.org/licenses/old-licenses/gpl-2.0.html**